Information Security Standard

Information Security Reviews Standard
Initially Approved: February 16, 2015
Revised: August 25, 2020 (as an Information Security Standard)
Revised: March 29, 2023
Administering Office: Office of the CIO

I. Standard Statement

This standard operates under University Policy 117 Information Security.

To ensure that information security is implemented and operated in accordance with policies and procedures, WCU's approach to managing information security and its implementation (i.e. policies, standards, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.

Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards, and any other security requirements.

Information systems shall be regularly reviewed for compliance with WCU's information security policies and standards.

II. Scope and Application

The scope of this standard addresses compliance with information security policies, standards and procedures and the review of information systems. It applies to the Division of Information Technology, the Office of Internal Audit, and all department managers at WCU.

III. Definitions

Technical compliance reviews - The examination of operational systems to ensure that hardware and software controls have been correctly implemented. This type of compliance review requires specialist technical expertise.

Penetration testing and vulnerability assessments - Provide a snapshot of a system in a specific state at a specific time which can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities. They might be carried out by independent experts specifically contracted for this purpose.

IV. Information Security Reviews Standard

a. Independent review of information security

An independent review is necessary to ensure the continuing suitability, adequacy, and effectiveness of WCU's approach to managing information security. The review should include assessing opportunities for improvement and the need for changes to the approach to security, including the policy and control objectives. Such a review should be carried out by individuals independent of the IT Division, e.g. the Office of Internal Audit or the North Carolina Office of the State Auditor or an external third-party organization specializing in such reviews. Individuals carrying out these reviews should have the appropriate skills and experience. The results of the independent review should be recorded and reported to the management who initiated the review and the Information Security and Privacy Governance Committee. These records should be maintained. If the independent review identifies inadequacies in the approach or implementation of information security, e.g. documented objectives and requirements are not met or not compliant with the direction for information security stated in the information security policies and standards, management should consider corrective actions.

b. Compliance with security policies and standards

Department managers are responsible for ensuring all workforce members complete any assigned information security training, and for enforcing computer and data security policies and standards. Managers should identify how to review and assess that information security requirements defined in policies, standards and other applicable regulations are met. If any non-compliance is found as a result of the review, managers should:

a) Identify the causes of the non-compliance;
b) Evaluate the need for actions to achieve compliance;
c) Implement appropriate corrective action;
d) Review the corrective action taken to verify its effectiveness and identify any deficiencies or weaknesses.

Results of reviews and corrective actions carried out by managers should be recorded and these records should be maintained. Managers should report the results to the persons carrying out independent reviews when an independent review takes place in the area of their responsibility.

c. Technical compliance review

Technical compliance should be reviewed, either by IT or as part of an independent review, preferably with the assistance of automated tools, which generate technical reports for subsequent interpretation by a technical specialist. Alternatively, manual reviews (supported by appropriate software tools, if necessary) by an experienced system engineer could be performed. If penetration tests or vulnerability assessments are used, caution should be exercised as such activities could lead to a compromise of the security of the system. Such tests should be planned, documented and repeatable. Any technical compliance review should only be carried out by competent, authorized persons or under the supervision of such persons.

Technical reviews of compliance with security policies and standards should include methods of reviewing those tools and components related to processing PII. This can include ongoing monitoring to verify that only permitted processing is taking place, and/or specific penetration or vulnerability tests.

V. Accountability and Enforcement

The Chancellor has established an Information Security and Privacy Governance Committee, which reports to the Chancellor. The charge of this Committee is to oversee the implementation of security policy, ensure procedures are up to date, coordinate all relevant security policy reviews, and assist offices with risk assessments, etc.

IT security personnel are responsible for overseeing regular reviews of information system activities to verify compliance with security policies, standards and procedures and identify risks to information assets.

The Office of Internal Audit or a designated third-party will periodically review policy and standard compliance.

Department managers are responsible for ensuring compliance with this standard and that any appropriate corrective action is taken, which may include the implementation of additional controls, employee training, and disciplinary action.

Failure to comply with this standard may result in the imposition of fines, or other significant penalties against WCU, and disciplinary action against employees.

VI. References

International Standards Organization (ISO/IEC 27002:2022, Clause 5 Organizational Controls)

University Policy 117 Information Security

45 CFR Part 164, Subpart C, Security and Privacy